Panel 3: The Applicability of International Law to Cyberspace & Characterization of Cyber Incidents

Catherine Lotrionte, co-chair, Eneken Tikk-Ringas, co-chair, Tom Dukes, Sean Kanuck

Discussion Points

'Cyber security' and the acceptable behavior of state and non-state actors in 'cyberspace' has become one of the centerpieces of international and national security talks. Calls for new legal instruments have been placed with international organizations by some states while others call for application of existing legal frameworks.

The core statement of this panel is that there is no 'cyber' framework per se from a legal perspective. There is, however, a substantive body of legal principles and norms, international and regional, to address different implications of uses of ICTs, such as how we establish and maintain relevant infrastructures, protocols and content; how we defend personal, corporate, national and international interests pertaining to uses of ICTs and how we balance interests involved under the contemporary paradigm of 'security'. Addressing 'the law of cyber security' therefore means addressing different legal authorities, instruments, concepts and practices some of which can and some of which cannot be applied simultaneously and all of which involve prerequisites to their applicability. Furthermore, these need to be addressed with the different national legal interpretations from various countries.

This panel will address legal principles, instruments and concepts applicable to uses of ICTs and the consequences of such use that do not rise to the threshold of 'use of force' and 'armed attack', thresholds to the applicability of the international laws related to conflict management to be addressed by the next panel. This panel will outline already existing normative approaches to telecommunications, crime/law enforcement, electronic transactions, privacy, espionage, etc and explain and discuss the relevance of such frameworks from state responsibility and government-level decision-making/strategy development perspective

The panel starts with a "legal threshold map" that would offer an outline of the main existing legal concepts and respective legal areas/thresholds/standards to get oriented in the applicability of already existing norms. The panel then outlines and discusses remedies available for pursuing one's interests in the cyber domain and resolving conflicts under the legal frameworks applicable to international telecommunications, data processing, computer-related crime and addresses the challenges related to balancing and co-applying such frameworks and concepts. It further elaborates on the law of state responsibility and how this area of law could be applied to cyber incidents. The discussion will focus on the incentives and considerations behind decisions to rely or not to rely on the existing legal instruments and the nature of the 'gaps' of implementation of law.

The panelists will address:

1) The practical vs. political need for and rationale behind the requests for new international legal instruments (e.g. the Russian and Chinese initiatives of the Code of Conduct, Draft Convention of Information Security and the UNODC cyber crime treaty initiative);
2) A 'legal' versus a 'policy' assessment of an incident and the choice of responses and remedies;
3) Categorization of cyber incidents under existing legal thresholds;
4) Identifying (potential) gaps in existing legal instruments and practice to be filled in by other normative (including non-binding) frameworks.